CLAIMS

I claim:

1. (Original) A system for secure data communications in at least one of Fax transmissions and computer network communications, comprising at least one of:
   a. A system that allows the sender to get a confirmation that the receiver received the message without having to rely on the receiver accessing a web site for reading the message.
   b. A system that enables the sender to prove that he indeed sent the message to the intended receiver at the specified time and date.
   c. A system that enables the sender to prove the content of the message that was sent.
   d. A system that enables the receiver to know that the message indeed originates from the purported sender without the need to rely on encryption and digital signatures.
   e. A system for preventing the theft of digital signatures based on a hardware that contains not only the encryption keys but also a surrounding processing in isolation so that malicious software cannot cheat the users by accessing said hardware.
   f. A system for preventing forgeries of source addresses of the senders of the messages which is applied to at least one of: the sender's phone number, the sender's email addresses, and the sender's IP addresses.

2. (Currently amended) The system of claim 1 wherein said communications are Fax transmissions, and <u>at least one of the following features exists:</u>
   a. The telephone company's computer identifies automatically Fax transmissions and adds its own identification of the originator's phone number to the transmission.
   b. <u>The telephone company's computer identifies automatically Fax transmissions and adds its own identification of the originator's phone number to the transmission, and said identification of the sender's phone number is transmitted directly to the receiving Fax machine by at least one of: 1. As part of the protocol or as additional protocol, so that the receiving Fax machine can understand this number and can</u>

itself add it to the Fax; 2.The phone company's computer adds it to the Fax transmission itself, so that it behaves like the first few pixel-lines or last few pixel-lines of the Fax transmission or is superimposed over any of the original pixel lines; 3.The receiving Fax can automatically identify the phone number of the sender like in identified phone calls, and can thus automatically add it to the printed Fax.

c. The sender has the option of disabling the sender's number identification.

d. If the sender disables phone number identification, the phone company still enforces at least a regional identification.

e. The confirmation that the fax was sent and/or that it was received is sent automatically by the phone company's computer.

3. (Cancelled).

4. (Currently amended) The system of claim 1 wherein said communications are Fax transmission and in order to confirm that the receiver indeed received the Fax, each Fax machine automatically sends back a confirmation Fax to the sender if the Fax was received OK, or does it at least if the sender requests it, and wherein said confirmation includes at least one of:

a. Sending back a copy of one or more or all of the received pages.

b. Sending back a serial number of the received Fax.

c. Sending back a digital key

d. Sending back a digital key based on a unique identifier of the receiving Fax and at least one of the time and date, the serial number of the message, and some identifier of the content.

e. The confirmation is done using the same connection that was dialed out by the sending fax.

5. (Cancelled).

6. (Cancelled).

7. (Currently amended) The system of claim 6 wherein said communications are Fax transmission and in order to confirm that the receiver indeed

received the Fax, the fax is sent through a trusted authority, and at least one of the following features exists:

a. Said authority automatically sends back to the sender, by at least one of fax and email, a confirmation of at least one of the intended receiver's identity, the time and date the Fax was sent, and the content of the Fax.
b. The trusted authority forwards the Fax to the receiver and makes sure that the receiver indeed received the Fax.
c. The trusted authority continues to attempt sending the Fax again at least for a number of times and/or for a certain time, until normal conventional confirmation is received from the receiving machine that the transmission went through OK and/or until confirmation is received, and/or until too much time has elapsed and/or too many attempts have failed.
d. The trusted authority keeps a copy of the fax in the authority's database, which can be retrieved upon request also later if needed.

8. (Original) The system of claim 1 wherein in order to ensure the safety of private keys a hardware that contains the private keys contains also all the software or firmware for accessing and processing these keys, so that in order to digitally sign and encrypt a document, the document has to be sent to this hardware and processed by the hardware itself, so the returned output from the hardware is the already encrypted and signed document.

9. (Original) The system of claim 8 wherein at least one of the following features exist:

a. Said hardware also uses at least one incrementally changing element, which can be affected also by the exact time and date, in order to reduce the chance of replay.
b. Said hardware has a secure and/or encrypted channel for accessing at least one of the computer screen and the printer and/or has an output means of its own, in order to display to the user the correct unencrypted document that is being signed.

c. Each authorization can be used only once and must therefore be explicitly reapplied in order to sign an additional document.
d. Using the hardware requires also typing some password or secret code.
e. The hardware can indicate at least the File size and/or CRC and/or other fingerprints of the file that is being signed, and at least one of a security software and a function of the Operating system and the user checks if the parameters displayed by the hardware fits with the parameters displayed by the computer.
f. At least one of a security software and the Operating System ensures that the users always sees the correct real document on which he is digitally signing, by preventing any other software from accessing the hardware and/or the driver and/or software that come with the hardware without explicit permission by the user.

10. (Original) The system of claim 1 wherein said communications are email messages and in order to prevent faking of the sender's email and/or his IP address, at least one of the following features is used:
    a. The mail server that receives the message from the user's computer can look at the "From" field and/or "reply-to" field of the e-mail message that the user is trying to send and refuse to relay the message if the "From field" indicates an email address who's corresponding IP address is beyond the range or list of allowed IP addresses for that server.
    b. The mail server that receives the message from the user's computer checks if the given sender e-mail address actually exists at all.
    c. Changing the e-mail protocol, so that each e-mail-sending program must use at least one of a random code and the exact time when the message was generated, and the email server immediately contacts back the sender and asks it to repeat the sent code and refuses to relay an e-mail message if the sender does not respond with the correct answer.
    d. Physical/Geographical IP addresses are used and each server can instantly know if any IP address given by the user is real or not according the trace of its route, and thus refuse to communicate with a

source that uses an IP address that is impossible according to its real position on the Internet.

e. The access provider and/or the e-mail server identify at least one of {the user's phone number, a unique identifier of the user's computer, a unique identifier of the user's communication card, the connection, and the IP address assigned to it for that connection} and therefore are able to prevent using a different IP address by the user's computer and/or using a stolen account by someone else.

f. The user has to explicitly notify the access provider of the sender email addresses that can be used from at least one of each uniquely identified computer and connection and phone numbers.

g. Each time a user's computer sends an email address or uses some IP address it is logged on the nearest access provider's node along with unique identifying data of the computer and/or the connection and/or the phone number used and/or the IP address that was assigned to this connection, and if the sender's email address changes more than a certain allowed number of times during that session then the offending messages can be blocked and/or logged.

h. The first server or node that the outgoing packets from the user's computer reaches first sends back a short package to the given source IP address and forwards the packets only if the machine at the given IP address confirms that it indeed initiated the outgoing packets.

i. Normal users that are not running servers are automatically marked by the access provider as end-node and thus attempts to pretend to be a server can be automatically ignored.

j. The mail server on the receiver's side verifies the IP of the sender's side server by contacting back the sender's side server, and even if the sending client can pretend to be a server, it doesn't help him since attempts to fake the IP address will not work.

11. (Original) The system of claim 1 wherein said communications are email messages and at least one of the following features exists:

a. Email servers or routers along the way are used for verifying the receipt of an email message.

b. At least the end-node email server or router that communicates directly with the final receiver can automatically send back a confirmation email to the sender if the email was received OK.
c. Confirmation can be sent also from relay servers or routers along the ways and not only the last one.

12. (Original) The system of claim 11 wherein said confirmation includes at least one of:
    a. Sending back a digitally certified copy of the email message and/or at least part of it.
    b. Sending back some serial number of the message.
    c. Sending back a digital key.
    d. Changing the email protocol so that the last server or router that communicates directly with the receiver can query the receiving node after sending the message and the receiving node either answers that it received it or that it didn't, and if no answer is received, the last sending node keeps trying at least for a certain number of times and/or a certain period.
    e. The original server of the sender or any other server along the way can send the request for acknowledgement to the receiving node and wait for the confirmation.
    f. The confirmation that the message was received OK by the receiving server includes sending also at least one CRC or fingerprint or size data together with the message from the sending server, so that the receiving server can confirm that the message came OK.
    g. The receiving server also sends back to the sending server a copy of the message it received, so that the sending server can check if it is identical with the sent message.
    h. A unique private key of the server prevents forgery of the receipt, so that knowing the secret key is required in order to be able to create the proper receipt at the given time and date.
    i. Sending back a return key that includes also at least one of CRC and fingerprints that can be used for confirming that what the content was.
    j. The server can save a copy of this CRC or CRCs or fingerprints at least upon request for at least a certain time period.

13. (Original) The system of claim 12 wherein said digital key is based on at least one of:
    a. A unique identifier of the server or router.
    b. The time and the date.
    c. The serial number of the message.
    d. At least one CRC and/or fingerprint that identifies the content of the message.

14. (Original) The system of claim 1 wherein said communications are email messages and a trusted authority is used, and no previous setting of account by the sender at the server is required, and each sender can use the services of the central authority by using a properly formed message, and said authority is used for confirming at least one of: The receipt of an email message, and The content of the message.

15. (Original) The system of claim 14 wherein said confirmation can be by at least one of:
    a. A certified copy return from the authority with at least one of a stamp or signature.
    b. In the form of a record kept at the authority for at least a few years, in case a later certificate is needed.
    c. A stamped return FAX.
    d. A digitally signed email.

16. (Cancelled).

17. (Original) The system of claim 14 wherein payments for the authority's services can be done by at least one of:
    a. Adding an appropriate header to the message that includes at least one of credit card info and micro-payments credit points.
    b. Payment later when the authority gets back to you.

c. Using a secure email protocol that contains unique parameters of the sender's computer or connection, in a way similar to a secure access to a web page.

d. Adding it automatically to the regular billing by the ISP.

18. (Currently amended) The system of claim 1 wherein at least one of the following features exists:

a. The sender can use any official sender and/or "reply-to" e-mail address that he wishes, but must include also an additional field which shows the correct e-mail address which was actually used during the sending of the message.

b. A user can specify sender email addresses that belong to another domain on the internet if the mail server on the site allows legitimate users to define various e-mails and/or IP addresses that they might use when actually sending the messages, and in order to enable this, if the outgoing mail server finds that the sender address is not within the allowed range, it can still relay the message by verifying with a server on that domain that the actual sender address is listed there.

c. Digital signatures cannot be used from IP addresses that are outside a range or list of allowed IP addresses.

d. When a confirmation is sent back to the user by a trusted authority or by servers along the way, the party that sends the confirmation also at least one of: Confirms that the sender indeed received the confirmation, and Is able to send again the confirmation if the sender requests it.

e. A trusted authority is used, which forwards the message to the receiver, and if the receiver has not received the message the trusted authority continues to attempt sending the message again at least for a number of times and/or for a certain time.

f. A copy of the message is sent in parallel also to a trusted authority for keeping a log of the content without the need to route the message through the authority, if other methods are used to sufficiently ensure that the message indeed has been received by the receiver.

g. The sending email server also adds its own confirmation key and/or time and date stamps and/or serial number, so that these can be used by the receiver as a confirmation about the content of the message that was sent to him.

h. The sending Fax machine also automatically adds is own unique serial number and/or key that preferably reflects also a time and date stamp, so that the receiver also has a confirmation that the fax sent to him was authentic.

i. The phone company's computer automatically identifies if the connection is used for a normal voice communication or for electronic data connection or Fax transmission, and then at least one of the following is done: 1. If it is a data connection the phone company forwards the number to the ISP even if the user has normally a block on identified phone calls when he initiates a normal voice call. 2.If it is a Fax or similar kind of transmission the phone company forwards the number to the called number even if the user has normally a block on identified phone calls when he initiates a normal voice call.

j. The sending server keeps a record of messages that were sent out, containing at least the subject, sender and receiver, at least for a certain period, and the receiving server and/or the user's client email program can be instructed by the user to check once in a while if and when any messages were sent from a certain sender or list of senders to the user.

k. The fax machine can be connected to the user's computer in a way that causes it to send the images of the faxed pages directly into the computer so that it can be send directly by email, without having to add a fax card to the computer itself and an additional phone line.

l. The fax machine can be connected to the user's computer in a way that causes it to send the images of the faxed pages directly into the computer so that it can be send directly by email, without having to add a fax card to the computer itself and an additional phone line, and this connection is done by connecting the fax to the parallel port or to the USB and adding a function to the fax that allows the user to send the fax-coded images to the computer instead of over phone lines, or dialing a special number that activates this.

m. A trusted authority is used and said authority saves at least one CRC and/or at least one fingerprint of the message which can be used for proving what the content was, without having to save the full content itself.

n. A trusted authority is used and said authority charges a smaller amount for saving only the CRC's and/or other fingerprints of the content, and charges larger amount for saving the full content.

19. (Cancelled).

20. (Original) The system of claim 1 wherein at least some combination with conventional postal services are used and wherein a certified email message or Fax is automatically relayed to a post-office branch which is near to the receiver's Physical address, and is printed and hand-delivered from there like an ordinary certified mail.

21. (Currently amended) The system of claim 20 wherein said near branch is found by at least one of:
    a. Using IP addresses that contain also physical addresses.
    b. Using the physical address of the receiver and automatically matching it with the near post office branch by at least one of country and city and zip code.

22. (Original) The system of claim 1 wherein at least some interchange is allowed between Fax and email messages, so that at least one of:
    a. Certified communications can be sent to the trusted authority for as email messages and converted there to Fax communications with the receiver.
    b. Certified communications can be sent to the trusted authority as Fax messages and converted there to email communications with the receiver.

23. (Currently amended) The system of claim 1 wherein at least one of the options of receipt-verification is used when at least one of:
    a. The user specifically requests certified communications.
    b. Automatically even without requesting it.
    c. Automatically for basic verification and based on user request for more intensive verification.
    d. Automatically for basic verification and based on user request for more intensive verification, wherein said basic verification includes sending back from the last server that communicates directly with the receiver at least a confirmation serial number and/or time and date stamp and/or digital key.

24-50 (Cancelled).

51. (Original) The system of claim 1 wherein the mail server at the side of the receiver can inform the mail server at the side of the sender, and/or the sender directly, if and when the receiver actually accessed the mail, by at least one of the following means:
    a. Sending a confirmation when the email client program actually downloads the message from the mail server at the side of the receiver.
    b. Keeping a log of said confirmation, at least for a certain period in order to enable the sender to request a copy of the confirmation also at a later time.
    c. At least one of a trusted authority, the mail server at the side of the receiver, and the sending mail server, encrypts the mail and sends in to the receiver and when the receiver wants to read the message, the opening key is download from the relevant server, thus confirming actual receipt, and said downloading is done when the message is received by the client program or when the user opens the message.
    d. The server saves at least also one or more fingerprints of the content and can send it back to the sender upon request.
    e. The email protocol is changed so that the receiving mail server has to send some kind of acknowledgement to the sending server any time

during the transmission of a message before the transmission is considered complete.

f. The sender and/or the sending server can also query the receiving mail server if the message has been downloaded by the receiver's client program.

g. The sending mail server and/or the receiving mail server automatically add an HTML code to the message that when executed makes the client mail program immediately connect to some address on the mail server, thus automatically confirming that the message has been opened.

52. (Cancelled).

53. (Original) The system of claim 51 wherein at least one of the following features exists:

a. If the receiving mail server is on a computer where the user gets the mail directly through logging in or through a mailbox web service, the receiving mail server informs the sender and/or the sending mail server that the message has been forwarded to the receiver at the moment that the servers adds the message to the user's messages Box.

b. The software that allows the user to access the message also sends a confirmation to the server when the user actually opens the mail message.

c. A resident software or driver ensures that the server is informed whenever the message is accessed, so that tempering with the client software cannot prevent notifying the server.

d. There is also a separate indication – if the user saw the header of the message even if he didn't open it, which is sent to the sender and/or to the sending mail server.

54. (Cancelled).

55. (Original) An email system wherein the user can instruct the receiving server and/or his email client to mark more conspicuously and/or put in a separate list all the emails from a list of senders which the user marks as preferred

and/or this group can be generated automatically by putting in the list all the emails to which the user himself sent messages and/or they are automatically given a higher position if the user sent more messages to them.

56. (Cancelled).

57. (Original) The system of claim 1 wherein in public-use computers the OS itself and/or a security software enables the administrator to specify that this is a public-use computer, and at least one of the following features exist:
    a. This setting can be changed only with the original installation disk and/or with a password and/or with some other physical key.
    b. When defined as a public computer, the OS and/or the security software indicates this in outgoing electronic communications.
    c. Any session-related traces are automatically removed by the system after a short time of inactivity and/or if the user does not re-enter a password chosen by the original person that started the session, or such traces are not saved at all.
    d. The OS and/or the security software allows the user to send additional email messages from the same session only if he know the password entered or chosen by the user when he started the session, etc.

58. (Cancelled).

59. (Cancelled).